UNITED STATES PATENT AND TRADEMARK OFFICE

NOTICE OF ALLOWANCE AND FEE(S) DUE

28653	7590	05/14/2009

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

EXAMINER
JEAN, FRANTZ B

ART UNIT	PAPER NUMBER
2454	

DATE MAILED: 05/14/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,660	03/17/2004	Conrad K. Herrmann	VIV/0014.01	2659

TITLE OF INVENTION: SYSTEM PROVIDING METHODOLOGY FOR ACCESS CONTROL WITH COOPERATIVE ENFORCEMENT

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	08/14/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Complete and send this form, together with applicable fee(s), to: <u>Mail</u>   **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or <u>Fax</u>   **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)	Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

28653   7590   05/14/2009

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

_____ (Depositor's name)

_____ (Signature)

_____ (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,660	03/17/2004	Conrad K. Herrmann	VIV/0014.01	2659

TITLE OF INVENTION: SYSTEM PROVIDING METHODOLOGY FOR ACCESS CONTROL WITH COOPERATIVE ENFORCEMENT

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	08/14/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
JEAN, FRANTZ B	2454	709-203000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE   (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) :   □ Individual   □ Corporation or other private group entity   □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.   □ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____   Date _____

Typed or printed name _____   Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,660	03/17/2004	Conrad K. Herrmann	VIV/0014.01	2659

			EXAMINER
28653	7590	05/14/2009	JEAN, FRANTZ B

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

ART UNIT	PAPER NUMBER
2454	

DATE MAILED: 05/14/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 1254 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 1254 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

	Application No.	Applicant(s)
Notice of Allowability	10/708,660	HERRMANN, CONRAD K.
	Examiner	Art Unit	
	Frantz B. Jean	2454	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment filed on 1/26/09.*

2. ☒ The allowed claim(s) is/are *1-68.*

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some* c) ☐ None of the:
       1. ☐ Certified copies of the priority documents have been received.
       2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
       3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of
      Paper No./Mail Date _____ .
   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____ .

/Frantz B. Jean/
Primary Examiner, Art Unit 2454

Claims 1- 68 are allowed over the prior art of record and in light of applicant's

arguments.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview

with John Smart on 4/12/09.

The application has been amended as follows: Please replace claims 1-68 with

the following:

1. (Currently amended) A method ~~for~~ employing supplemental authentication to prevent
an inadequately secured client from compromising a host that offers a service that the client
wishes to access ~~authorizing a client to access a service based on compliance with a policy
required for access to the service~~, the method comprising:
    ~~specifying a policy required for access to the service, the policy including security-
relevant requirements that the client must meet before the client is provided access to the service;~~
    specifying a supplemental authentication policy to be enforced upon the client's request
to access the service, the policy establishing firewall and anti-virus measures required to be
installed and operational at the client in order for the client to be considered adequately secured
for accessing the service;
    receiving ~~detecting~~ a request for access to the service from the client;
    attempting primary authentication of the client based on credentials presented by the
client;
    if the client ~~is authenticated based on the credentials~~ passes primary authentication,
attempting secondary authentication ~~determining whether the client is in compliance with said~~

~~policy based~~ by testing the client's current firewall and anti-virus measures against said policy to confirm that the client is adequately secured for accessing the service ~~based, at least in part, on attributes of the client~~; and

if the client ~~is determined to be in compliance with said policy~~ fails to pass both primary and secondary authentications, ~~providing~~ denying the client access to the service.

2. (Original) The method of claim 1, wherein the service comprises a remote service accessible by the client through a network.

3. (Original) The method of claim 1, further comprising:
restricting access to the service if the client is determined to be non-compliant with said policy.

4. (Original) The method of claim 3, wherein restricting access includes assigning limited access privileges to the client.

5. (Original) The method of claim 3, wherein restricting access includes issuing a Kerberos ticket specifying limited access privileges if the client is determined to be non-compliant with the policy.

6. (Original) The method of claim 1, wherein said policy comprises a security policy.

7. (Original) The method of claim 6, wherein said security policy includes security measures required on the client.

8. (Currently amended) The method of claim 1, wherein said policy includes ~~anti-virus~~ anti-spyware measures required on the client.

9. (Original) The method of claim 1, wherein said step of providing access includes issuing a Kerberos ticket specifying access privileges provided to the client.

10. (Currently amended) The method of claim 1, wherein ~~attributes of the client include~~ the policy further specifies that a selected one of a file integrity policy be in effect at the client, a file be installed at the client, a process be running at the client, a particular checksum value exist at the client, and a particular registry entry exist at the client.

11. (Currently amended) The method of claim 1, wherein said ~~detecting~~ receiving step includes ~~detecting~~ receiving a request for access to a server by a remote client.

12. (Currently amended) The method of claim 1, wherein said ~~detecting~~ receiving step includes ~~detecting~~ receiving a request for access to a service on a computer system by another process on the computer system.

13. (Currently amended) The method of claim 1, wherein said attempting primary authentication step includes authentication based on user identity.

14. (Currently amended) The method of claim 1, wherein said attempting primary authentication step includes using a selected one of Kerberos authentication, Pluggable Authentication Module (PAM) authentication, Extensible Authentication Protocol (EAP) authentication, Generic Security Service API (GSS-API) authentication, and trust negotiation in TLS (TNT) authentication.

15. (Original) The method of claim 1, wherein said credentials include a selected one of a user name, a password, and a certificate.

16. (Currently amended) The method of claim 1, wherein said attempting secondary authentication ~~determining~~ step includes obtaining ~~attribute~~ firewall and anti-virus information from the client.

17. (Currently amended) The method of claim 16, wherein said step of obtaining firewall

and anti-virus information from the client includes requesting ~~attribute~~ firewall and anti-virus
information collected by a client-side component.

18. (Currently amended) The method of claim 1, wherein said attempting secondary
authentication ~~determining~~ step includes substeps of:

    providing a copy of the policy to the client; and

    performing a compliance check at the client to determine compliance with the policy.

19. (Currently amended) The method of claim 1, wherein said attempting secondary
authentication ~~determining~~ step includes obtaining information from a security evaluation service
that has previously evaluated compliance by the client with the policy.

20. (Previously presented) A computer-readable storage medium having processor-
executable instructions for performing the method of claim 1.

21. (Original) A downloadable set of processor-executable instructions for performing
the method of claim 1.

22. (Currently amended) A system ~~for authenticating and assigning access privileges to a
client device for~~ providing supplemental authentication to prevent an inadequately secured client
device from compromising a host that offers access to a service, the system comprising:

    a supplemental authentication policy specifying access privileges to be assigned to a
client device based on security-related attributes of the client device that are relevant to the
~~client's~~ client device's access of the service, said policy establishing firewall and anti-virus
measures required to be installed and operational at the client device in order for the client device
to be considered adequately secured to access the service;

    a primary authentication module for receiving a request from a given client device for
access to the service and determining whether to authenticate the given client device for access
to the service, wherein the given client device is denied access to the service if the primary
authentication module cannot authenticate the device; and

a supplemental authentication module for examining <u>current security-related</u> attributes of
~~a~~ <u>the given</u> client device authenticated by said primary authentication module and ~~assigning~~
~~access privileges to~~ <u>determining whether to authenticate</u> the <u>given</u> client device <u>by testing</u>
<u>whether the given client device's current firewall and anti-virus measures satisfy said policy</u>
~~based on the policy~~<u>, wherein the given client device is denied access to the service if the</u>
<u>supplemental authentication module cannot authenticate the device</u>.

23. (Original) The system of claim 22, wherein said policy comprises a security policy.

24. (Original) The system of claim 22, wherein said policy includes security attributes of
the client device.

25. (Currently amended) The system of claim 22, wherein said ~~step of examining~~
~~attributes of the client device includes determining~~ <u>supplemental authentication module</u>
<u>determines</u> whether specified anti-virus measures are in effect on the client device.

26. (Currently amended) The system of claim 22, wherein said ~~step of examining~~
~~attributes of the client device includes examining~~ <u>supplemental authentication module examines</u>
a selected one of a file integrity policy in effect at the client device, a file installed at the client
device, a process running at the client device, a particular checksum value at the client device,
and a registry entry at the client device.

27. (Original) The system of claim 22, wherein said primary authentication module uses
a selected one of Kerberos authentication, Pluggable Authentication Module (PAM)
authentication, Extensible Authentication Protocol (EAP) authentication, Generic Security
Service API (GSS-API) authentication, and trust negotiation in TLS (TNT) authentication.

28. (Original) The system of claim 22, wherein said primary authentication module
authenticates the client device based upon user identity.

29. (Original) The system of claim 28, wherein the client device provides a user name and password to said primary authentication module for authenticating user identity.

30. (Original) The system of claim 28, wherein the client device provides a digital certificate to said primary authentication module for authenticating user identity.

31. (Currently amended) The system of claim 22, wherein the supplemental authentication module includes a component on the client device for collecting ~~attribute~~ information about firewall and anti-virus measures.

32. (Currently amended) The system of claim 31, wherein the component on the client device evaluates the collected ~~attribute~~ information about firewall and anti-virus measures at the client device for determining compliance of the client device with the policy.

33. (Original) The system of claim 32, further comprising:
a policy server for providing the policy to the client device.

34. (Currently amended) The system of claim 22, wherein the supplemental authentication module receives information about ~~attributes~~ firewall and anti-virus measures of the client device from the client device.

35. (Currently amended) The system of claim 34, wherein the client device provides ~~attribute~~ information about firewall and anti-virus measures to the supplemental authentication module in response to a message from the supplemental authentication module.

36. (Currently amended) The system of claim 35, wherein said ~~attribute~~ information about firewall and anti-virus measures is provided as a selected one of a text string, an Extensible Markup Language (XML) document, and an Abstract Syntax Notation One (ASN.1) file.

37. (Original) The system of claim 22, wherein the supplemental authentication module

permits access to the service if the client device is in compliance with the policy.

38. (Original) The system of claim 22, wherein the supplemental authentication module issues a Kerberos ticket specifying the client device's access privileges.

39. (Original) The system of claim 22, wherein the supplemental authentication module restricts access to the service if the client device is non-compliant with the policy.

40. (Original) The system of claim 22, further comprising:

a policy server in communication with the supplemental authentication module for evaluating compliance by the client device with the policy based upon attributes of the client device.

41. (Original) The system of claim 22, wherein the supplemental authentication module comprises a selected one of an anti-virus engine, a configuration checker, and a security engine.

42. (Currently amended) A method ~~for assigning privileges to a client to use a service based on an access policy~~ providing supplemental authentication to prevent an inadequately secured client from compromising a host that offers a service that the client wishes to access, the method comprising:

specifying ~~an~~ a supplemental authentication access policy for assigning privileges to a client to use the service based on security attributes of the client, the policy ~~including security-relevant requirements that the client must meet before the client is provided access to the service~~ establishing firewall and anti-virus measures required to be installed and operational at the client in order for the client to be considered adequately secured for accessing the service;

receiving ~~detecting~~ a request for use of the service from a client;

attempting primary authentication of the client based on user identity information provided by the client;

if the client is authenticated based on user identity, ~~collecting attribute information from the client~~ attempting supplemental authentication by testing whether the client's current firewall

and anti-virus measures satisfy said policy; and

assigning privileges to the client to use the service based on ~~the collected attribute information and the access policy~~ whether the client's firewall and anti-virus measures satisfy said policy, so that the client is denied access to the service if insufficient privileges are assigned.

43. (Original) The method of claim 42, wherein said step of assigning privileges includes blocking access to the service if the client is determined to be non-compliant with the access policy.

44. (Original) The method of claim 42, wherein said step of assigning privileges includes restricting access to the service if the client is determined to be non-compliant with the access policy.

45. (Original) The method of claim 42, wherein set step of assigning privileges includes issuing a Kerberos ticket to the client.

46. (Original) The method of claim 42, wherein said access policy includes security measures required on the client.

47. (Currently amended) The method of claim 42, wherein said access policy includes ~~anti-virus~~ anti-spyware measures required on the client.

48. (Original) The method of claim 42, wherein said access policy includes an attribute required for the client.

49. (Original) The method of claim 48, wherein said attribute includes a selected one of a file integrity policy in effect at the client, a file installed at the client, a process running at the client, a particular checksum value at the client, and a registry entry at the client.

50. (Currently amended) The method of claim 42, wherein said ~~detecting~~ receiving step

includes ~~detecting~~ receiving a request for access to a server by a remote client.

51.   (Currently amended) The method of claim 42, wherein said ~~collecting~~ attempting supplemental authentication step includes requesting attribute information from the client.

52.   (Original) The method of claim 51, wherein the attribute information is provided as a selected one of a text string, an Extensible Markup Language (XML) document, and an Abstract Syntax Notation One (ASN.1) file.

53.   (Currently amended) The method of claim 42, wherein said ~~collecting~~ attempting supplemental authentication step includes using a client-side component for collecting attribute information.

54.   (Original) The method of claim 53, wherein said client-side component determines whether the client is in compliance with the access policy based on the collected attribute information.

55.   (Original) The method of claim 53, wherein said client-side component sends the collected attribute information to a policy server for determining whether the client is in compliance with the access policy.

56.   (Previously presented) A computer-readable storage medium having processor-executable instructions for performing the method of claim 42.

57.   (Original) A downloadable set of processor-executable instructions for performing the method of claim 42.

58.   (Currently amended) In a system comprising a client computer connecting to a service through a network, a method for regulating access to the service based on a specified supplemental authentication access policy, the policy including ~~security-relevant~~ requirements

about ~~firewall and anti-virus measures~~ that the client computer must meet before the client computer is provided access to the service, the method comprising:

after initial authentication of the client computer has occurred, attempting supplemental authentication of the client computer by transmitting a challenge from the service to the client computer connecting to the service to determine whether the client computer's current firewall and anti-virus measures satisfy the requirements of said policy ~~for determining whether the client computer is in compliance with said specified access policy, wherein said access policy includes attributes of the client computer that are acceptable for permitting access to the service~~;

transmitting a response from the client computer back to the service, for responding to the challenge issued by the service that is attempting supplemental authentication of the client computer; and

based on the response received from the client computer, blocking access to the service by the client computer if the client ~~computer~~ computer's current firewall and anti-virus measures fail to satisfy the requirements of said policy ~~does not respond appropriately to the challenge issued by the service~~.

59. (Original) The method of claim 58, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

60. (Original) The method of claim 58, wherein said challenge includes at least some rules of said access policy that are transmitted to the client computer.

61. (Original) The method of claim 58, wherein said access policy is provided at the client computer.

62. (Original) The method of claim 61, wherein the client computer performs a compliance check for determining compliance with the access policy and returns the compliance check result in response to the challenge.

63. (Currently amended) The method of claim 58, wherein said ~~attributes include~~ policy

<u>further specifies that</u> a selected one of a file integrity policy <u>be</u> in effect at the client computer, a file <u>be</u> installed at the client computer, a process <u>be</u> running at the client computer, a particular checksum value <u>exist</u> at the client computer, and a <u>particular</u> registry entry <u>exist</u> at the client computer.

    64. (Original) The method of claim 58, further comprising:
otherwise, permitting access to the service by the client computer.

    65. (Original) The method of claim 64, wherein permitting the client computer to access the service includes assigning access privileges based on the response received from the client computer.

    66. (Original) The method of claim 65, wherein assigning access privileges includes issuing a Kerberos ticket for providing said access privileges to the client computer.

    67. (Original) A downloadable set of processor-executable instructions for performing the method of claim 58.

    68. (Previously presented) A computer-readable storage medium having processor-executable instructions for performing the method of claim 58.

    The following is an examiner's statement of reasons for allowance: <u>specifying a supplemental authentication policy to be enforced upon the client's request to access the service, the policy establishing firewall and anti-virus measures required to be installed and operational at the client in order for the client to be considered adequately secured for accessing the service;</u>
    <u>receiving</u> a request for access to the service from the client; attempting <u>primary</u> authentication of the client based on credentials presented by the client; if the client ~~is authenticated based on the credentials~~ <u>passes primary authentication,</u> attempting <u>secondary</u> authentication <u>by testing the client's current firewall and anti-virus measures against said policy to confirm that the client is adequately secured for accessing the service</u> ~~based, at least in part, on~~

~~attributes of the client~~; and if the client <u>fails to pass both primary and secondary authentications,</u> ~~providing~~ <u>denying the client</u> access to the service.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Frantz B. Jean whose telephone number is 571-272-3937. The examiner can normally be reached on 8:30-6:00 M-f.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan J. Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Frantz B. Jean/
Primary Examiner, Art Unit 2454